Cybersecurity: Current Legislation, Executive Branch Initiatives, and Options for Congress

Catherine A. Theohary
Analyst in National Security Policy and Information Operations

John Rollins
Specialist in Terrorism and National Security

September 30, 2009

Congressional Research Service
7-5700
www.crs.gov
R40836

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
30 SEP 2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Cybersecurity: Current Legislation, Executive Branch Initiatives, and Options for Congress	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Congressional Research Service,Library of Congress,Washington,DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**26**	

Summary

Increasing focus on current cyber threats to federal information technology systems, nonfederal critical information infrastructure, and other nonfederal systems has led to numerous legislative cybersecurity proposals and executive branch initiatives. The proposed National Defense Authorization Act for Fiscal Year 2010 (NDAA FY2010) and the Intelligence Authorization Act for Fiscal Year 2010 (IIA FY2010) both contain provisions that would affect programs and funding for current and future cybersecurity-related programs. In May 2009, the Obama Administration issued its 60-day review of cybersecurity policy, declaring that U.S. information networks would be treated as a strategic national asset.

There is no single congressional committee or executive agency with primary responsibility over all aspects of cybersecurity; each entity involved pursues cybersecurity from a limited vantage point dictated by committee jurisdiction. Many different initiatives exist, but because of fragmentation of missions and responsibilities, "stove-piping," and a lack of mutual awareness between stakeholders, it is difficult to ascertain where there may be programmatic overlap or gaps in cybersecurity policy.

Drawing from common themes found in the Comprehensive National Cybersecurity Initiative (CNCI), a study by the Center for Strategic and International Studies (CSIS) Commission for the 44th Presidency, and the proposed near-term action plan from the President's recent Cyberspace Policy Review, this report identifies priority areas in cybersecurity for policy consideration. The report then lists and synopsizes current legislation that has been developed to address various aspects of the cybersecurity problem. It then lists the current status of the legislation and compares legislation with existing executive branch initiatives. Finally, analysis of information contained in executive branch initiatives and congressional legislation is used to offer cybersecurity-related considerations for Congress.

Contents

Tables

Appendixes

Contacts

Introduction

Comprehensively addressing national cybersecurity-related issues is a difficult task because of a number of technical and policy considerations. A persistent set of issues has stymied significant progress in detecting and deterring existing threats and implementing effective safeguard measures.[1] Issues that appear to continually challenge U.S. cybersecurity efforts include

- uncertainty of the geographic location of the perpetrators of cyber attacks;
- the evolving integration of mobile technology devices into critical information infrastructure;
- the introduction of new vulnerabilities to the nation's infrastructure from increasingly sophisticated threats;
- a poorly coordinated federal-private sector approach to addressing emerging risks; and
- legal ambiguities with respect to U.S. response and offensive actions.

While the ever-changing nature of modern technological devices is often noted as a complicating factor in securing the nation's telecommunications and cyber infrastructure, many security observers suggest that an equally daunting group of strategy and policy challenges must be addressed if the United States is to continue to rely on technology as a major component of societal activities. Since 2008, a number of strategy and policy proposals have been offered that may assist in addressing the appropriate balance of relying on emerging technology and network-centric governance while safeguarding critical infrastructure and control systems, as well as privacy and civil liberty considerations.

Recent events such as the April 2007 cyber attacks on Estonia and cyber attacks during the 2008 Georgian incursion have served to increase awareness that cybersecurity is not just about protecting computers, but also has implications for U.S. national security and economic well-being. The Obama Administration declared that U.S. critical information infrastructures are a strategic national asset in a May 29, 2009, speech by the President.[2] Recognizing the importance of cyberspace over the past few years, both the legislative and executive branches of government have developed cybersecurity legislation and related initiatives, respectively. However, just as there is no single congressional committee that can claim primary jurisdiction over cyberspace, neither is there a single executive agency or department with sole cybersecurity responsibility or commensurate authorities. As the President stated, "No single official oversees cybersecurity policy across the federal government, and no single agency has the responsibility or authority to match the scope and scale of the challenge. Indeed, when it comes to cybersecurity, federal agencies have overlapping missions and don't coordinate and communicate nearly as well as they should—with each other or with the private sector."[3]

[1] For background in cyber vulnerabilities, see archived CRS Report RL33123, *Terrorist Capabilities for Cyberattack: Overview and Policy Issues*, by John Rollins and Clay Wilson.

[2] White House Office of the Press Secretary, "Remarks by the President on Securing our Nation's Cyber Infrastructure," press release, May 29, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

[3] Ibid.

Cybersecurity is a cross-cutting field that affects many government and non-governmental stakeholders. As such, one of the most basic concerns, but most difficult to address, is that the term itself can carry different connotations for the various entities. For example, the U.S. military views cyberspace as a warfighting domain as well as a force enabler, enhancing troops' ability to operate in real-time and with improved situational awareness. For the Department of Defense, cybersecurity takes on an offensive or defensive national security role. For other government stakeholders, cybersecurity means information security, or securing the information that resides on cyber infrastructure such as telecommunications networks, or the processes these networks enable. And for some, cybersecurity means protecting the information infrastructure from a physical or electronic attack.

Research Methodology

For purposes of this report, cybersecurity is broadly defined as the protection of critical information infrastructure and its processes and content. This report does not discuss reorganizing the executive branch to better address cybersecurity-related issues, nor does it discuss the military's role in securing federal cyber networks. The report presents the emerging issues in cybersecurity as identified by the Comprehensive National Cybersecurity Initiative (CNCI), the Center for Strategic and International Studies (CSIS) Report to the 44th President, and the Obama Administration's 60-day policy review report, and groups common themes into broad subject areas. These issues are compared to the current statutory framework, new legislative efforts in the 111th Congress, and executive branch initiatives to identify commonalities and possible gaps.

Federal executive branch programs, strategy documents, and reports have been analyzed to illustrate the government's response to emerging challenges in cybersecurity. It should be noted that some of the apparent gaps discovered may actually be addressed by existing classified programs, which cannot be discussed in this unclassified report.

Difficulties in Addressing Cybersecurity Issues

Conceptual and definitional differences among agencies make a unified government strategic approach to cybersecurity a difficult challenge to coordinate. For the Department of Defense, cybersecurity is both the protection of its own networks, processes and content—sometimes referred to as "information assurance"—as well as enabling the freedom of movement to fight and win battles in cyberspace. This approach differs from that of the Department of Homeland Security (DHS), which is tasked to coordinate cybersecurity between the rest of the federal government and the private sector. DHS's task is complicated, as cyberspace technology and processes are largely owned and operated by the private sector, and as the authority of the federal government to exert control over cybersecurity activities may be limited. Some point to the 2003 National Strategy to Secure Cyberspace as a framework for organizing and prioritizing federal cybersecurity efforts, including the private sector. However, others note that this document fails to take into account the rapid rate of change in technologies or fails to offer a comprehensive strategy for combating current threats and anticipating future threats.

At the operational level, some security observers are concerned about the federal government's present ability to first detect and then respond in a coordinated way to a cyber incident of major significance. Agencies may have their own response plans, procedures, and responsible entities that vastly differ from those of other cooperating agencies. The Cyber Incident Annex to the

National Response Plan of December 2004 describes many different authorities and policy documents to guide a response, as well as many different organizations that must communicate effectively in the event of a crisis. Multiple federal information systems enterprise networks make a concerted strategic approach to network security even more difficult, in that each has its own authentication procedures and security standards.

Another cybersecurity difficulty for the government is balancing the protection of civil liberties and individual privacy protections with the desire for comprehensive security of networks and information. It is difficult to secure information infrastructures and their content without tradeoffs between security and the freedoms associated with the Internet. Many concerned about civil liberties fear that the executive branch will use its national security powers and national defense mandate as justification for encroaching on privacy without adequate oversight. Others regard security measures, such as network traffic monitoring, as a violation of the Universal Declaration of Human Rights, which states that "no one shall be subjected to arbitrary interference with his privacy, family, home or correspondence."[4] Complicating the issue is a lack of consensus on the definition of "privacy" in the context of the Internet, and a lack of consensus on what sort of government resolution may be necessary as a network security measure.

Recent Initiatives Addressing U.S. Cybersecurity Concerns

Since 2008, numerous executive branch, legislative, and think tank recommendations and proposals have been offered to address various aspects of ongoing and emerging cybersecurity issues. The Comprehensive National Cybersecurity Initiative (CNCI), the Center for Strategic and International Studies (CSIS) Commission on Cybersecurity for the 44th Presidency,[5] and the White House 60-Day Cyberspace Policy Review (commonly referred to as the 60-Day Cyber Security Review)[6] are the most current attempts to frame the issue and are often referred to when discussions arise regarding how best to identify challenges and implement changes to the current U.S. approach to cybersecurity.

The Comprehensive National Cybersecurity Initiative

In January 2008, the Bush Administration initiated the Comprehensive National Cybersecurity Initiative (CNCI) in an effort to make the United States more secure against cyber threats. The Homeland Security Presidential Directive 23 and National Security Presidential Directive 54 establishing the CNCI are classified, although some details of the initiative have been made public through departmental press releases, speeches by executive branch leaders, and analysis offered by individuals who follow cybersecurity- and terrorism-related issues.

Reportedly, the CNCI "establishes the policy, strategy, and guidelines to secure federal systems."[7] The CNCI also delineates "an approach that anticipates future cyber threats and technologies, and

[4] Article 12 of the Universal Declaration of Human Rights, accessed at http://www.un.org/en/documents/udhr/.

[5] CSIS Commission on Cybersecurity for the 44th Presidency, *Securing Cyberspace for the 44th Presidency*, December 2008, http://www.csis.org/tech/cyber/.

[6] The White House, *Cyberspace Policy Review*, May 29, 2009, http://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf.

[7] Department of Homeland Security, *Fact Sheet: DHS End-of-Year Accomplishments*, December 18, 2008, http://www.dhs.gov/xnews/releases/pr_1229609413187.shtm.

requires the federal government to integrate many of its technical and organizational capabilities to better address sophisticated threats and vulnerabilities."[8] Rather than serving as an overarching national strategy document with specific instructions for federal agency implementation activities, the CNCI is seen as a plan of action for programs and initiatives to be addressed at the operational and tactical level. Given the classified nature of the presidential directives and the secrecy accompanying department and agency activities related to this issues, few details are known about CNCI-related federal government implementation efforts. According to one media account, Steven Chabinsky, Deputy Director of the Joint Interagency Cyber Task Force for the Office of the Director of National Intelligence, stated at an information technology security conference that there are 12 objectives supporting the initiative's goal of comprehensively addressing the nation's cyber security concerns.[9] These include the following:

1. Move toward managing a single federal enterprise network (an integrated communications system architecture for the federal government with common security standards across the network).
2. Deploy intrinsic detection systems.
3. Develop and deploy intrusion prevention tools.
4. Review and potentially redirect research and funding.
5. Connect current government cyber operations centers.
6. Develop a government-wide cyber intelligence plan.
7. Increase the security of classified networks.
8. Expand cyber education.
9. Define enduring leap-ahead technologies (investing in high-risk, high-reward research and development to ensure transformational change).
10. Define enduring deterrent technologies and programs.
11. Develop multi-pronged approaches to supply chain risk management (potential tampering within the production line and the risk associated with computer products and parts made outside the United States).
12. Define the role of cybersecurity in private sector domains.

Commission on Cybersecurity for the 44th Presidency

A Cybersecurity Commission (the Commission) organized by the Center for Strategic and International Studies (CSIS) was formed in 2008 to provide advice to the new Administration on the creation and maintenance of a comprehensive cybersecurity strategy. In a December 2008 report, the Commission provided findings and recommendations to secure cyberspace during the 44th presidency and to help inform policymaking. The following actions were proposed in the report as areas requiring priority attention:

- create a comprehensive national cybersecurity strategy;

[8] Department of Homeland Security, *Department Responsibilities: Maximize Use of Science, Technology and Innovation*, http://www.dhs.gov/xabout/gc_1244659918636.shtm.

[9] Jill R. Aitoro, "National Cyber Security Initiative will have a dozen parts," *NextGov*, August 1, 2008.

- lead from the White House;
- reinvent public-private partnership;
- regulate cyberspace;
- authenticate digital identities;
- modernize legal authorities;
- use acquisitions to improve security;
- build capabilities through research training and education.

Obama Administration 60-Day Cyberspace Policy Review

On May 29, 2009, President Obama issued the results of the Administration's 60-Day Cyberspace Policy Review (60-day review). Following the issuance of the CNCI, the review's goal was to assess U.S. policies and organizational structures for cybersecurity. In order to develop a strategic framework to ensure that the U.S. government's initiatives are appropriately integrated, resourced, and coordinated, the following near-term action plan issues were noted in the 60-day review:

- Appoint a cybersecurity official to coordinate interagency strategy and policy.
- Prepare and update national strategy to secure the information and communications infrastructure.
- Designate cybersecurity as one of the President's key management priorities and establish performance metrics.
- Designate a privacy and civil liberties official in the NSC cybersecurity directorate.
- Convene appropriate interagency mechanisms to conduct legal analysis of priority cybersecurity issues.[10]
- Initiate a national cybersecurity public awareness and education campaign.
- Develop U.S. government positions for an international cybersecurity policy framework.
- Prepare a cybersecurity incident response plan.
- Develop a framework for research and development strategies that focus on "game-changing" technologies that enhance security.
- Build a cybersecurity-based identity management vision and strategy that addresses privacy and civil liberties interests.

[10] For additional information and analysis regarding potential legal considerations of cybersecurity related issues, see CRS Report R40427, *Comprehensive National Cybersecurity Initiative: Legal Authorities and Policy Considerations*, by John Rollins and Anna C. Henning.

Common Themes of Recent Cybersecurity Initiatives

Some common themes begin to emerge from the initiatives and recommendations suggested in CNCI, the CSIS report, and the 60-day review. These themes are broadly captured under the following headings:

National cybersecurity strategy—conceptualizing a current comprehensive approach toward a government-wide cybersecurity solution, outlining ends, ways, and means along with a prioritization of effort.

Executive branch organization—reorganizing existing executive branch structures, or standing up new entities to coordinate cybersecurity throughout the interagency process.

Congressional oversight concerns—identifying committee jurisdictions to oversee budgetary priorities and goals for cybersecurity programs.

Establish/update legal authorities—expanding and/or clarifying roles and responsibilities of cybersecurity stakeholders.

Privacy and civil liberties—maintaining privacy and freedom of speech protections on the Internet while devising cybersecurity procedures.

Awareness, research, education, and training—developing a workforce to meet cybersecurity goals, raising citizenry awareness of cybersecurity best practices, and developing more secure technologies.

Outreach, collaboration, and policy formation—working across government and with the private sector to share information on threats and other data, and to develop shared approaches to securing cyberspace.

These broad themes are used to compare current policy and legislative proposals with executive branch initiatives. A description of selected executive branch initiatives is followed by a comparison matrix that illustrates trends in cybersecurity efforts.

Representative Sampling of Preexisting Executive Branch Programs and Initiatives

Upon release of the Administration's 60-day review, President Obama announced the creation of a new cabinet-level position to coordinate cybersecurity strategy and policy across the federal government. This new "Cyber Coordinator," sometimes referred to as a "Cyber Czar," is to report to the National Security Advisor and the Director of the National Economic Council. As of September 2009, the position has not been filled.

Programs in several departments address various aspects of cybersecurity within their respective areas of responsibility. While every department and agency has an individual and collective role in securing federal cyber enterprises, some organizations have appeared to have greater authority and capability than others. A few of the departments and their accompanying responsibilities are noted below.

The Department of Commerce's National Institute of Standards and Technology (NIST) has primary responsibility for reducing cyber vulnerabilities in the electrical grid. In the Energy Independence and Security Act of 2007 (EISA; P.L. 110-139), Congress directed NIST to lead the Department of Energy and other agencies in ensuring an interoperable, secure, and open energy infrastructure that will enable all electric resources to contribute to an efficient and reliable electricity network. Specifically, EISA gave NIST "primary responsibility to coordinate development of a framework that includes protocols and model standards for information management to achieve interoperability of smart grid devices and systems." Cybersecurity and associated standards are being addressed as part of this Smart Grid Interoperability Framework that is under development.[11] NIST is also tasked to promote the development of key security standards and guidelines to support the implementation of and compliance with the Federal Information Security Management Act of 2002 (FISMA; P.L. 107-347).[12]

The Department of Health and Human Services (HHS) has recently adopted new interoperability standards for health care information technology. HHS is responsible for implementing privacy and security standards for electronic personal health information.[13]

The Department of Homeland Security (DHS) leads the cybersecurity coordination for non-military departments and agencies in the federal government. The National Cyber Security Directorate works with private industry on a voluntary basis to promote safe cybersecurity practices. DHS is also home to the National Cyber Security Center, a clearinghouse whose mission is to coordinate information from all agencies to help secure cyber networks and systems, foster collaboration, and improve situational awareness.

The Department of Defense (DOD) has a number of programs designed to address vulnerabilities and threats to its own networks. Secretary Gates recently announced the creation of a new sub-unified command under the U.S. Strategic Command, to be called U.S. Cyber Command (CYBERCOM). This new command is to coordinate a unified approach to defending and securing military cyber networks. The December 2006 National Military Strategy for Cyberspace Operations (NMS-CO) guides computer network attack and defense principles. The Defense Industrial Base (DIB) initiative provides a vehicle through which DOD and industry partners can better share information on cyber threats and defense practices. DOD also has established a Cybercrime Center (DC3) that assists in criminal, counterintelligence, counterterrorism, and fraud investigations by the Defense Criminal Investigative Organizations (DCIOs) and DOD counterintelligence activities. In addition to setting forensics standards, it provides training and testing laboratories for protection of defense information systems.

Common themes often noted by many cybersecurity experts underscore a lack of transparency and dearth of defined departmental roles and responsibilities in addressing cyber-related issues from a comprehensive national approach. Such concerns often assert that a continuation of addressing cyber incidents as a myopic individual agency responsibility will eventually lead to increased systemic national vulnerabilities and put the nation at greater risk. It is argued by some

[11] Testimony of Cita M. Furlani, Director Information Technology Laboratory, National Institute of Standards and Technology, United States Department of Commerce, Before the House Committee on Homeland Security Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, United States House of Representatives July 21, 2009.

[12] See CRS Report RL32357, *Computer Security: A Summary of Selected Federal Laws, Executive Orders, and Presidential Directives*, by John D. Moteff.

[13] See CRS Report RS20934, *A Brief Summary of the HIPAA Medical Privacy Rule*, by Gina Stevens.

that a more strategic approach to detecting, identifying, mitigating, and responding to future cyber incidences may strengthen both the individual agency and the whole-of-government approach to securing the technologies that underpin every aspect of modern society.

Comparison Matrix

The following table is designed to assist in identifying emerging cybersecurity themes contained within previously enumerated respective executive branch activities, including both Administration-led initiatives, federal agency programs, statutes, and proposed legislation. While the issue contained in the applicable legislation and executive branch initiatives do not always perfectly align (based on the number of issues addressed and the degree of specificity), **Table 1** notes corresponding legislation proposed in both the 111th Congress and the 110th Congress to relevant existing statutory frameworks. Finally, current appropriations bills are shown to illustrate congressional spending priorities. Overview lists and summaries of the cybersecurity-related legislation are found in the **Appendix**.

Table 1. Comparison of Emerging Cybersecurity Themes

Emerging Issues	Executive Branch Activity	111th Congress	110th Congress	Statutory Framework
National Cybersecurity Strategy	CNCI; 60-Day Review; 2003 NSSC; NMS-CO	S. 773		44 U.S.C. § 3541; 18 U.S.C. § 1030
Executive Branch Organization	Cyber Coordinator; CYBERCOM; DHS NCC, NCSD	H.R. 1174; H.R. 1910; S. 921; H.R. 2165; H.R. 2195; S. 778;		
Congressional Oversight Concerns		S. 1494; S. 1438		
Establish/Update Legal Authorities		S. 773; S. 946		
Privacy and Civil Liberties	HHS Rules	H.R. 1		42 USC § 201; 18 U.S.C. § 1030
Awareness, Research, Education, Training	DOD Cybercrime Center; DHS NCC	H.R. 2200; H.R. 2454; S. 177; S. 1391; H.R. 2647; H.R. 2892; H.R. 266; H.R. 1	H.R. 1; H.R. 4986; H.R. 2764; H.R. 2638	
Outreach, Collaboration and Policy Formation	Cyber Coordinator; DIB Initiative; NIST standards	S. 1436; H.R. 2020; H.R. 1	H.R. 6	
Appropriations		H.R. 3293; H.R. 2892	H.J.Res. 20	

A common theme emerging from a review of the current proposals is the need for a current comprehensive national cybersecurity strategy. The most recent strategy, the 2003 National Strategy to Secure Cyberspace, outlined a unified, whole-of-government approach to dealing with cybersecurity.[14] Some say that the 2003 policy has not kept pace with the rapidly evolving technologies and threats in cyberspace, and have called upon the Administration to craft [15]a new national cybersecurity strategy with the assistance of Congress. Others say it is not a comprehensive strategy but is instead a set of recommendations, much like the CSIS Commission report. The Administration's 60-day review's near-term action plan calls for preparing and updating a new national strategy for securing communications and information infrastructure.

From the table, the legislative branch appears to share this concern; legislation proposed in S. 733 calls upon the President to present a national strategy within one year of the bill's enactment. This bill would also create a national advisory panel to oversee implementation of the strategic plan and to periodically advise the president on the need for revising the strategy. Some have criticized the provision, which would give the President emergency control over public and private networks in the event of a crisis, and have argued that the bill is vague in addressing civil liberties protections. As this legislation is marked up, alternative proposals may be considered.

Another area of interest is executive branch organization. As the federal government continues to organize to defend its strategic cyber assets, some Members of Congress have proposed legislation that would create new offices or positions, or give greater authority and direction to existing positions. It is unclear how proposals such as S. 778 to establish the Office of the National Cybersecurity Advisor within the Executive Office of the President fits with the administration's recently proposed Cyber Coordinator, a cabinet position that will report to both the National Security Advisor and the Director of the National Economic Council.[16]

Privacy and civil liberties concerns appear to be lacking in recent congressional proposals. However, there are Internet privacy and non-disclosure policies written into statutory frameworks that may not specifically address cybersecurity, such as the Health Insurance Portability and Accountability Act (HIPAA; P.L. 104-191) and personal health care information safeguards, or the Gramm-Leach-Bliley Act (P.L. 106-102) and financial information for corporations or individuals. Civil liberties is an area of concern for both Congress and privacy advocates, but does not appear to be an immediate priority reflected in legislative action to date. This may suggest to some that existing programs have emphasized securing networks before tackling the attendant issues such as freedom of speech, privacy, and civil liberty protections as they pertain to the Internet.

Upon review of the legislation contained in **Table 1**, another common area of focus appears to be addressing issues related to workforce development, outreach, and collaboration-based initiatives. The proposed S. 733 in its initial version contained provisions for presidential cybersecurity authorities. Rewrites of this legislation reportedly may revise this provision.[17] Such activities

[14] George W. Bush, *The National Strategy to Secure Cyberspace*, (Washington, D.C.: The White House, February 2003) http://www.dhs.gov/xlibrary/assets/National_Cyberspace_Strategy.pdf.

[15] Declan McCullagh, "Bill would give president emergency control of Internet," *CNet News*, August 28, 2009, pp. http://news.cnet.com/8301-13578_3-10320096-38.html.

[16] White House Office of the Press Secretary, "Remarks by the President on Securing our Nation's Cyber Infrastructure," press release, May 29, 2009, http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/.

[17] David Sessions, "Cybersecurity Bill Gives President Broad Powers Over Internet," *PoliticsDaily*, August 31, 2009, (continued...)

could be replaced or supplemented with the inclusion of additional focus on the training, education, and research aspects of cybersecurity.

Considerations and Options for Congress

Questions of resources and appropriate organizational structures appear to dominate legislative and executive branch efforts and proposals for federal cybersecurity programs. However, the lack of a current and clearly articulated national strategy remains a concern to some. Without an overall government strategy and underlying policies to outline cybersecurity priorities, goals, and how to achieve them, executive organization and program funding may be a muddled process. Congress may consider drafting legislation that would outline a strategic security framework and priority areas for the Obama Administration to address. With the advent of a new strategy, Congress may then wish to review the authorization and appropriations legislation for cybersecurity related programs for possible mission duplication and adherence to strategic goals.

Reportedly, the Homeland Security and Governmental Affairs Committee, recognizing calls for lawmakers to combine efforts, is to work with the Armed Services, Commerce, Intelligence and Judiciary panels to craft comprehensive cybersecurity legislation.[18] In addition to the options and recommendations contained in the legislative proposals, CNCI, White House 60-Day Cyber Security Review, and the Commission on Cybersecurity for the 44th Presidency reports, Congress may wish to consider other options when addressing current and emerging cyber risks to the nation. Additional options may include the following:

- Drafting legislation, strategy, and policies that take into account rapidly changing telecommunications and Internet-based technologies.
- Ensuring risk reduction education and training is a core component for all federal government employee performance assessments, with an advanced course provided to individuals who spend a majority of their work time undertaking technology-related activities.
- Requiring the National Intelligence Council to produce classified and unclassified annual reports addressing current and emerging cyber-related based threats.
- Requiring the Department of Homeland Security annually to produce cybersecurity risk assessments for all nonfederal government entities with security responsibilities. The assessments could address issues relating to current and emerging threats, current best security practices, and mitigation and remediation recommendations, as well as provide a venue for the recipients of this report to submit threat information and requests for assistance to the Department.
- Legislatively defining U.S. cyber offensive and defensive responsibilities and authorities.

(...continued)

http://www.politicsdaily.com/2009/08/31/cybersecurity-bill-gives-president-broad-powers-over-internet/.

[18] Gautham Nagesh, "Lawmakers join forces on cybersecurity legislation," September 14, 2009, p. http://www.nextgov.com/nextgov/ng_20090914_5789.php?oref=topstory.

- Establishing a permanent Congressional Commission or Task Force that would assess and report to Congress successes and ongoing challenges in U.S. cybersecurity programs and activities.
- Drafting legislation to mandate privacy and freedom of speech protections to be incorporated into a national strategy.
- Assessing current congressional committee jurisdiction.

Appendix. Cybersecurity-Related Legislation in the 111th and 110th Congresses

This appendix provides an overview list of legislative proposals in the 111th Congress, followed by a brief summary of the related section. Following this is an overview list of legislation that was proposed in the 110th Congress, indicating legislative initiatives extending back into the previous Administration. The final section of the appendix summarizes existing statutory foundations in cybersecurity. These lists are not exhaustive, but rather are designed to give a representative overview of cybersecurity related activities in the federal government and to assist in identifying priority areas where legislation may be necessary.

This information is current as of September 28, 2009. For the most up-to-date information, please consult the Legislative Information System (LIS) at http://www.congress.gov/.

Overview list of Bills in the 111th Congress that Address a Cybersecurity-Related Issue

Directly tied to cybersecurity

S. 1438 Fostering a Global Response to Cyber Attacks Act (referred to Senate committee).

H.R. 266 Cybersecurity Education Enhancement Act of 2009 (referred to House subcommittee)—expansion of professional cybersecurity education programs.

S. 778 To establish, within the Executive Office of the President, the Office of the National Cybersecurity Advisor (referred to Senate committee).

S. 773 Cybersecurity Act of 2009 (referred to Senate committee).

Cybersecurity components as part of broader legislation

H.R. 2195 To amend the Federal Power Act to provide additional authorities to adequately protect the critical electric infrastructure against cyber attack, and for other purposes (referred to House subcommittee)—protection of electric infrastructure from cyber attack.

H.R. 2165 Bulk Power System Protection Act of 2009 (referred to House committee)—to amend Part II of the Federal Power Act to address known cybersecurity threats to the reliability of the bulk power system, and to provide emergency authority to address future cybersecurity threats to the reliability of the bulk power system.

S. 921 United States Information and Communications Enhancement Act of 2009 (referred to Senate committee)—creation of the National Office for Cyberspace.

H.R. 2868 Chemical Facility Anti-Terrorism Act of 2009 (referred to House committee)—several sections mention cybersecurity in connection with overall security for chemical facilities.

S. 1494 Intelligence Authorization Act for Fiscal Year 2010 (passed/agreed to in Senate)—has an extensive and detailed section (340) on cybersecurity oversight.

H.R. 1910 Chief Technology Officer Act of 2009 (referred to House subcommittee)—to create the Office of the Chief Technology Officer within the Executive Office of the President.

Tied via appropriations or authorization

H.R. 2892 Department of Homeland Security Appropriations Act, 2010 (awaiting conference)—"$1,700,000 shall be for the Center for Counterterrorism and Cyber Crime."

H.R. 2647 National Defense Authorization Act for Fiscal Year 2010 (awaiting conference)—civilian cybersecurity training authorization, creation of Joint Program Office for Cyber Operations Capabilities.

S. 1391 Department of Defense Authorization Act for Fiscal Year 2010 (awaiting conference)—civilian cybersecurity training authorization.

Peripheral cybersecurity related or mentions

P.L. 111-5 (H.R. 1) American Recovery and Reinvestment Act, 2009—under Title XXX Health Information Technology and Quality, section 13001 directs privacy standards for electronic health information.

Title VI directs the Commerce Department and the Federal Communications Commission (FCC) to institute and expand the "broadband technologies and opportunities program."

S. 177 Strengthening Our Economy Through Small Business Innovation Act of 2009 (referred to Senate committee)—cybersecurity mentioned as a research priority for small businesses.

H.R. 1131 Community Protection and Response Act of 2009 (referred to House subcommittee)—includes a cyber attack in the listing of major disaster.

H.R. 1174 FEMA Independence Act of 2009 (referred to House subcommittee)—an Assistant Secretary for Cybersecurity is mentioned for an independent FEMA.

H.R. 2454 American Clean Energy and Security Act of 2009 (placed on calendar in Senate)—cybersecurity mentioned as a concern.

H.R. 2200 Transportation Security Administration Authorization Act (referred to Senate committee after being received from House)—mentions a cyber attack as a security concern.

S. 1436 Energy and Water Development and Related Agencies Appropriations Act, 2010 (placed on Calendar in Senate)—for the "purpose of forming and governing a national energy sector cyber organization that have the knowledge and capacity to focus cybersecurity research and development and to identify and disseminate best practices; organize the collection, analysis and dissemination of infrastructure vulnerabilities and threats; work cooperatively with the Department of Energy and other federal agencies to identify areas where federal agencies with jurisdiction may best support efforts to enhance security of the bulk power electric grid."

H.R. 3293 Departments of Labor, Health and Human Services, and Education, and Related Agencies Appropriations Act, 2010 (placed on calendar in Senate)—provides $607,482,000 for the public health and social services emergency fund "to support activities related to countering

potential biological, nuclear, radiological, chemical, and cybersecurity threats to civilian populations."

Details on Bills in the 111th Congress that Address a Cybersecurity-Related Issue

H.R. 2892 Department of Homeland Security Appropriations Act, 2010

Status of bill: Awaiting conference.

See under: Title III—Protection, Preparedness, Response, and Recovery; infrastructure protection and information security.

See under: Title III—Protection, Preparedness, Response, and Recovery; Federal Emergency Management Agency; State and local programs; item 12 (B).

Summary: The bill would allocate $1,700,000 for the Center for Counterterrorism and Cyber Crime, located in Norwich University, Northfield, Vermont.

H.R. 2454 American Clean Energy and Security Act of 2009

Status of bill: Placed on Calendar in Senate.

See under: Section 216 A—Transmission Planning. Subsection on "objectives" (1), under "Federal Policy" (a).

Summary: One of the objectives of the mentioned "federal policy" is to provide cybersecurity for the regional electrical grid.

H.R. 3293 Departments of Labor, Health and Human Services, and Education, and Related Agencies Appropriations Act, 2010

Status of bill: Placed on Calendar in Senate.

See under: Title II—Office of the Secretary, public health and social services emergency fund.

Summary: Provides $607,482,000 for the public health and social services emergency fund to support activities related to countering potential threats to civilian populations, among them, cybersecurity related threats. Cybersecurity threats are mentioned together with biological, nuclear, radiological, and chemical threats.

S. 1436 Energy and Water Development and Related Agencies Appropriations Act, 2010

Status of bill: Placed on Calendar in Senate.

See under: Title III—Department of Energy; Energy Programs; Electricity Delivery and Energy Reliability.

Summary: The section would allocate funding for the Department of Energy as it relates to electricity delivery and energy reliability. As part of the funding the Secretary must establish an

"independent national energy sector cyber security organization to institute research, development and deployment priorities, including policies and protocol to ensure the effective deployment of tested and validated technology and software controls to protect the bulk power electric grid and integration of smart grid technology to enhance the security of the electricity grid."

H.R. 2200 Transportation Security Administration Authorization Act

Status of bill: Referred to Senate Committee after being received from House.

See under: Title I—Authorization of Appropriations; Section 102. Risk-Based System for Allocation of Resources; Assessment and Prioritization of Risks.

Summary: The section would require TSA to implement a system of risk-based allocation of resources and provide a report that includes "a summary that ranks the risks within and across transportation modes, including vulnerability of a cyber attack."

H.R. 1910 Chief Technology Officer Act of 2009

Status of bill: Introduced in House—referred to House Subcommittee on Information Policy, Consensus, and National Archives.

See under: Section 2—Office of the Chief Technology Officer; Policy Planning, Analysis and Advice.

Summary: The bill would create the office of the Chief Technology Officer within the Executive Office of the President. Section 2 would require the Chief Technology Officer to assess the impact of information technology and networked information technology systems and applications on cybersecurity and personal privacy and advise the President on steps necessary to mitigate and manage security and privacy risks.

Beyond this specific cybersecurity concern, the CTO would also be responsible for "fact-gathering, analysis, and assessment of the federal government's information technology infrastructures, information technology strategy, and use of information technology." Other responsibilities would be ensuring "the security and privacy of the federal information technology infrastructure and networks" and "coordinating closely with other federal departments and agencies having responsibilities regarding security and privacy of the infrastructure and networks."

H.R. 1174 FEMA Independence Act of 2009

Status of bill: Introduced in House—referred to House Subcommittee on Emergency Communications, Preparedness, and Response.

See under: Title V—Other Offices and Functions; Section 514.

Summary: The section would create an "Assistant Secretary for Cybersecurity and Communications" as part of an independent FEMA.

H.R. 1131 Community Protection and Response Act of 2009

Status of bill: Introduced in House—referred to House Subcommittee on Early Childhood, Elementary, and Secondary Education.

See under: Section 3—Definition of Major Disaster.

Summary: The section would amend the Disaster Relief and Emergency Assistance Act to improve federal response efforts after a terrorist strike or other major disaster affecting homeland security. In the section for the definition of a major disaster it would include cyber attack on computer systems as one of the possibilities under "terrorist attack."

S. 177 Strengthening Our Economy Through Small Business Innovation Act of 2009

Status of bill: Introduced in Senate—referred to Senate Committee on Small Business and Entrepreneurship.

See under: Section 6—Inclusion of Energy, Security, Transportation, And Water Related Research In The List of Topics Deserving Special Consideration As SBIR Research Topics.

Summary: The bill would extend allocation of funds for research programs related to the Small Business Innovation Research program. Section 6 includes cybersecurity as one of the topics of interest, in particular the research by the National Academy of Sciences relating to cybersecurity.

S. 1391 Department of Defense Authorization Act for Fiscal Year 2010

Status of bill: Awaiting conference.

See under: Title IX—Department of Defense Organization and Management; Subtitle D—Other Matters; Section 932—Instruction of Private Sector Employees in Cyber Security Courses of the Defense Cyber Investigations Training Academy.

Summary: The bill provides authority for the Secretary of Defense to permit private sector employees to enroll in and receive instruction at the Defense Cyber Investigations Training Academy. No more than 200 full-time student positions may be filled at any one time by private sector employees enrolled under this section. Eligible private sector employees will be those engaged in providing significant defense related support to the Department of Defense or other federal agencies or those whose work product is relevant to national security policy or strategy.

In addition to the above section (932)—section 1222 "Report on Cuba and Cuba's Relations With Other Countries" includes "the status and extent of Cuba's cyberwarfare program" as one of the seven subjects to be addressed by the report on Cuba required from the Director of National Intelligence.

H.R. 2647 National Defense Authorization Act for Fiscal Year 2010

Status of bill: Awaiting conference.

See under: Title IX—Department of Defense Organization and Management; Subtitle D—Other Matters; Section 932—Instruction of Private Sector Employees in Cyber Security Courses of the Defense Cyber Investigations Training Academy.

Summary: The bill provides authority for the Secretary of Defense to permit private sector employees to enroll in and receive instruction at the Defense Cyber Investigations Training Academy. No more than 200 full-time student positions may be filled at any one time by private sector employees enrolled under this section. Eligible private sector employees will be those engaged in providing significant defense related support to the Department of Defense or other federal agencies or those whose work product is relevant to national security policy or strategy.

In addition to the above section (932)—section 1222 "Report on Cuba and Cuba's Relations With Other Countries" includes "the status and extent of Cuba's cyberwarfare program" as one of the seven subjects to be addressed by the report required from the Director of National Intelligence on Cuba.

S. 1494 Intelligence Authorization Act for Fiscal Year 2010

Status of bill: Passed/agreed to in Senate.

See under: Title III—General Intelligence Community Matters; Subtitle D—Congressional Oversight, Plans, and Reports; Section 340 – Cybersecurity Oversight.

Summary: Section 340 would improve congressional oversight of federal cybersecurity programs. S. 1494 would require that the President inform Congress about every cybersecurity program currently in operation and every new program created thereafter. The program notification must include some type of certification on the legality of the program as well as an assessment on the program's privacy impact.

H.R. 2868 Chemical Facility Anti-Terrorism Act of 2009

Status of bill: Introduced in House—referred to House Committee on the Judiciary.

See under: Title XXI – Regulations of Security Practices at Chemical Facilities; Section 2101—Definitions.

Summary: The bill defines "chemical facility security performance standards" as including the deterrence of cyber sabotage, "including by preventing unauthorized onsite or remote access to critical process controls." Later in the bill, cybersecurity is mentioned several times alongside physical security as seemingly equally important for the overall security of chemical facilities.

S. 921 United States Information and Communications Enhancement Act of 2009

Status of bill: Introduced in Senate—referred to Senate Committee on Homeland Security and Governmental Affairs.

See under: Subchapter II—Information Security; Subsection 3552—National Office for Cyberspace.

Summary: S. 921 would establish the National Office for Cyberspace within the Executive Office of the President. The Director of the National Office for Cyberspace is tasked with developing and implementing a comprehensive national cyberspace strategy. The Office would play a crucial role in deterring cyber attacks and defending the cyber critical infrastructure.

H.R. 2165 Bulk Power System Protection Act of 2009

Status of bill: Introduced in House—referred to House Committee on Energy and Commerce.

See under: Section 3—Protection of Bulk Power System From Cybersecurity Threats.

Summary: The bill seeks to amend Part II of the Federal Power Act in order to address cybersecurity threats to the reliability of the bulk power system. In addition, the Federal Energy Regulatory Commission would be authorized to respond in cases of imminent cyber security threats. The section also emphasizes ensuring that the Commission protects cybersecurity-related information.

H.R. 2195 To amend the Federal Power Act to provide additional authorities to adequately protect the critical electric infrastructure against cyber attack, and for other purposes

Status of bill: Introduced in House—referred to House Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology.

See under: Section 224—Critical Infrastructure; Part B—Assessment, Report, and Determination.

Summary: The bill attempts to improve the cybersecurity of the critical electric infrastructure through added powers and responsibilities for the Secretary of Homeland Security as well as the Federal Energy Regulatory Commission. Beyond assessing the cyber threats to the critical electric infrastructure, the Secretary of Homeland Security would be required to initiate several interim measures to protect the system from cyber attack. The Secretary of Homeland Security would then produce periodic assessments on the vulnerabilities and threats to the critical electric infrastructure and provide those to Congress as well as to the Federal Energy Regulatory Commission.

S. 773 Cybersecurity Act of 2009

Status of bill: Introduced in Senate—referred to Senate Committee on Commerce, Science, and Transportation.

See under: Section 3—Cybersecurity Advisory Panel.

Summary: Section 3 would instruct the President to designate a Cybersecurity Advisory Panel.

See under: Section 4—Real-Time Cybersecurity Dashboard.

Summary: Section 4 would require the Secretary of Commerce to implement a system to provide dynamic and real-time cybersecurity status and vulnerability information for all federal government information systems and networks managed by the Department of Commerce.

See under: Section 5—State and Regional Cybersecurity Enhancement Program; Part A—Creation and Support of Cybersecurity Centers.

Summary: The section would require the Secretary of Commerce to provide assistance for the creation and support of Regional Cybersecurity Centers in order to promote and implement cybersecurity standards at the state and regional levels.

See under: Section 6—NIST Standards Development and Compliance.

Summary: The section would require the National Institute of Standards and Technology to establish measurable security cybersecurity standards for all federal government, government contractor, or grantee critical infrastructure information systems and networks in the following areas: cybersecurity metrics research, security controls, and software security.

See under: Section 7—Licensing and Certification of Cybersecurity Professionals.

Summary: The section would require the Secretary of Commerce to develop and integrate a national licensing, certification, and periodic recertification program for cybersecurity professionals.

See under: Section 11—Federal Cybersecurity Research and Development.

Summary: The section would require the Director of the National Science Foundation to give priority to computer, information science, and engineering research to ensure support is provided to meet cybersecurity challenges.

See under: Section 18—Cybersecurity Responsibilities and Authority.

Summary: The section would require the President to develop and implement a comprehensive national cybersecurity strategy that includes such thigs as a long-term plan of the nation's cybersecurity future as well as a Quadrennial Cyber Review.

S. 778 To establish, within the Executive Office of the President, the Office of the National Cybersecurity Advisor

Status of bill: Introduced in Senate—referred to Senate Committee on Homeland Security and Governmental Affairs.

See under: Section 1—Office of the National Cybersecurity Advisor.

Summary: The bill would establish an Office of the National Cybersecurity Advisor within the Executive Office of the President. The position would serve the President as the principal advisor for all cybersecurity related matters.

H.R. 266 Cybersecurity Education Enhancement Act of 2009

Status of bill: Introduced in House—referred to the Subcommittee on Higher Education, Lifelong Learning, and Competitiveness.

See under: Section 2—Department of Homeland Security Cybersecurity Training Programs and Equipment.

Summary: The bill would authorize the Secretary of Homeland Security to establish a program to award grants to institutions of higher education for the establishment or expansion of cybersecurity professional development programs.

S. 1438 Fostering a Global Response to Cyber Attacks Act

Status of bill: Introduced in Senate—referred to Senate Committee on Foreign Relations.

See under: Section 4—Report On Improving Cybersecurity.

Summary: The bill expresses the interest of Congress is improving the nation's cybersecurity overall. Section 4 would require the Secretary of State to submit to the Senate and House a report describing "any actions taken by the United States to work with the governments of foreign countries to improve cybersecurity."

Procurement

Title XLI—Procurement (in thousands of dollars)

Under "Procurement—Defense Wide": Major Equipment DISA #027—Cyber Security Initiative $18,188.

Under "Operational Systems Development" for the Navy: # 0301372N Cyber Security Initiative GDIP unknown amount (classified).

Under "Research, Development, Test & Evaluation, Air Force": Cybersecurity for control networks research $4,000.

Under "Operational Systems Development"—Airforce: #0305103F Cybersecurity initiative $2,065.

Under "RDT&E" Defense-wide: # 0305103E Cybersecurity initiative $30,400.

Under "Operational Systems Development" Defense-wide: # 0301371G Cybersecurity initiative CCP unknown amount (classified).

Under "Operational Systems Development" Defense-wide: # 0301372L Cybersecurity initiative GDIP unknown amount (classified).

Under "Operational Systems Development" Defense-wide: # 0305103D8Z Cybersecurity initiative $993.

Under "Operational Systems Development" Defense-wide: # 0305103G Cybersecurity initiative unknown amount (classified).

Under "Operational Systems Development" Defense-wide: # 0305103K Cybersecurity initiative $10,080.

Title XLVI—Department of Energy National Security Programs

Under "Cyber security": $122,511.

Overview of Bills in the 110th Congress that Address(ed) a Cybersecurity-Related Issue

Passed bills—public law

P.L. 110-5 (H.J.Res. 20) Revised Continuing Appropriations Resolution, 2007. Provides $43,075,000 for "cybersecurity" activities for DOE.

P.L. 110-53 (H.R. 1) Implementing Recommendations of the 9/11 Commission Act of 2007. Creates an Under Secretary responsible for overseeing critical infrastructure protection, cybersecurity, and other related programs of the Department.

Also, creates R&D program that can "research technologies that mitigate damages in the event of a cyber attack."

P.L. 110-139 (H.R. 6) Energy Independence and Security Act of 2007. Mandates that the "smart grid" must incorporate "full cybersecurity."

P.L. 110-181 (H.R. 4986) National Defense Authorization Act for Fiscal Year 2008. Indicates that the annual report on the military power of the People's Republic of China must include "developments in China's asymmetric capabilities, including efforts to acquire, develop, and deploy cyberwarfare capabilities."

Section 1814 requires the Secretary of Defense to prepare a plan for response to natural disasters and terrorist events—including a "cyber attack'' as one of the scenarios that must be included in the plans.

Section 3123 includes cybersecurity threats as part of the "plan for addressing security risks posed to nuclear weapons complex."

P.L. 110-161 (H.R. 2764) Consolidated Appropriations Act, 2008. Includes $143,539,000 in FBI salaries and expenses to "address emerging threats in counterterrorism and cybersecurity."

P.L. 110-329 (H.R. 2638) Consolidated Security, Disaster Assistance, and Continuing Appropriations Act, 2009. Provides the Department of Homeland Security with $806,913,000 for "necessary expenses for infrastructure protection and information security programs and activities" including $3,500,000 for State and local cybersecurity training; and $4,000,000 for the Power and Cyber Systems Protection, Analysis, and Testing Program at the Idaho National Laboratory.

Bills that did not become law

H.R. 263 Cybersecurity Education Enhancement Act of 2008. Would have directed the Secretary of Homeland Security, acting through the Assistant Secretary of Cybersecurity, to establish a program awarding competitive grants to institutions of higher education for (1) cybersecurity professional development programs, (2) associate degree programs in cybersecurity, and (3) the purchase of equipment to provide training in cybersecurity for professional development and degree programs. (CRS summary)

Final status: Reported by the Committee on Homeland Security.

H.R. 4791 Federal Agency Data Protection Act. In section 4, under the "authority of Director of Office of Management and Budget to establish information security policies and procedures," it would have required agencies comply with a "minimally acceptable system configuration requirements consistent with best practices, including checklists developed under section 8(c) of the Cyber Security Research and Development Act (P.L. 107-305; 116 Stat. 2378) by the Director of the National Institute of Standards and Technology."

Final status: Referred to Senate Committee after being Received from House.

H.R. 5959 Intelligence Authorization Act for Fiscal Year 2009. Bill called for the President to create a "comprehensive national cybersecurity initiative advisory panel" that would be composed of representatives of Congress, the executive branch, and the private sector to report on information security for the federal government, critical infrastructure, among other issues.

Final status: Placed on Calendar in Senate.

H.R. 7007 National Commission on American Cybersecurity Act of 2008. The bill would have established the "American Cybersecurity Commission" to investigate the current threats to the cybersecurity of American business and infrastructure from foreign entities. The commission would have focused on "strategy for American business, national infrastructure, and United States Government non-military and non-national security related computer systems."

Final status: Introduced in House.

Summary list of Statutory Foundations for Cybersecurity Legislation

44 U.S.C. § 3541 Federal Information Security Management Act of 2002

Status of bill: P.L. 107-347 on December 17, 2002.

See under: Title III of the E-Government Act of 2002.

Summary: Contains standards for securing information and information systems within federal agencies, and requires compliance reports be submitted to the Office of Management and Budget (OMB).

18 U.S.C. § 2510 Electronic Communications Privacy Act of 1986

Status of bill: P.L. 99-508 100 Stat. 1848, October 21, 1986.

See under: Titles I and II of the ECPA.

Summary: Title I of the ECPA protects wire, oral, and electronic communications while in transit. It sets down requirements for search warrants that are more stringent than in other settings. Title II of the ECPA, the Stored Communications Act (SCA) protects communication held in electronic storage, most notably messages stored on computers.

18 U.S.C. § 1030 Computer Fraud and Abuse Act of 1984

Status of bill: P.L. 98-473, 98 Stat. 2190 on October 12, 1984.

Summary: Defines criminality of security breaches and unauthorized access to data on federal computer systems and certain financial institutions.

42 USC § 201 The Health Insurance Portability and Accountability Act of 1996 (HIPAA)

Status of bill: P.L. 104-191, 110 Stat. 1936.

See under: 45CFR164.501—Privacy rule.

Summary: Protects the privacy of individually identifiable health information in computerized insurance records.

15 U.S.C. § 6801 Financial Services Modernization Act of 1999 (Gramm-Leach-Bliley)

Status of bill: P.L. 106-102, 113 Stat. 1338, enacted November 12, 1999.

See under: Disclosure of Nonpublic Personal Information (Financial Privacy Rule).

Summary: Requires financial institutions to provide consumers with a privacy notice at the time the consumer relationship is established and annually thereafter. The privacy notice must explain the information collected about the consumer, where that information is shared, how that information is used, how that information is protected, and the option to opt-out of sharing with third-party companies.

Author Contact Information

Catherine A. Theohary
Analyst in National Security Policy and Information Operations
ctheohary@crs.loc.gov, 7-0844

John Rollins
Specialist in Terrorism and National Security
jrollins@crs.loc.gov, 7-5529